AMENDMENTS TO THE SPECIFICATION

Please amend the Specification as follows:

On page 4, amend ¶ [0014] as follows:

[0014] An arrangement consistent with this convention is depicted in FIG. 1. Therein a server system 11 comprises a server computer 110 on which there is installed a server application (server) 111. Server 111 may, when executed, provide a predetermined service to authorized client systems. As depicted in FIG. 1, a client system 12 comprises a client computer 120 on which there is installed a client application (client) [[112]] 121. Server system 11 is coupled to client system 12 through a communications link 13. Although not specifically illustrated as such, communications link 13 may include the Internet. In the configuration of FIG. 1, server computer 110, www.acme.com, for example, may include an FTP (file transfer protocol) server 111 that listens on a well-known port 112, i.e., tcp/21. Client 121 typically knows that in order to access (receive FTP files from) server 111 on server comparator 110, port tcp/21 on www.acme.com must be accessed.

On page 11, amend ¶ [0041] as follows:

[0041] In the embodiments described above, a high level of security may be established by a one-step mapping procedure in which there is initially provided a decoy port number. A table, accessible to, or included with, both the client and the server, maps the decoy port number to a valid port number. In other embodiments, an even greater level of security may be gained by first using a table, such as has been described above, to map a decoy port number to an intermediate port number. Subsequent processing, which may involve [[on]] one or more additional steps, maps the intermediate port number to a valid port number. The subsequent processing may take advantage of, or be based on, information or mechanisms that are known to both the server and to the client. However, the information or mechanism used for the subsequent processing from the intermediate port number to the valid port number may, or may not, be also available to others. However, unauthorized individuals or entities will not be privy to the manner in which that information is used to generate valid port numbers from decoy port numbers or from intermediate port numbers.